UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/746,305	12/21/2000	Kevin L. Wiley	062891.0424 (IOS 2392)	1828

7590 12/22/2004

Terry J. Stalford
Baker Botts L.L.P.
2001 Ross Avenue
Dallas, TX 75201-2980

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/746,305	**Applicant(s)** WILEY ET AL.	
	Examiner Christopher A. Revak	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspond nce address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2000*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *50,51* is/are allowed.

6)☒ Claim(s) *1-16,18,19,21-37,39-43,45 and 47-49* is/are rejected.

7)☒ Claim(s) *17,20,38,44 and 46* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 December 2000* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-16,18,19,21-37,39-43,45, and 47-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S. Patent 5,850,516 in view of Conklin et al, U.S. Patent 5,991,881.

As per claims 1,21, and 39, Schneier discloses of a method and system for maintaining network activity data for an intrusion detection system (col. 3, lines 5-16). Data representative of network activity is stored in attack tree structures (datasets) is stored in a database (col. 5, lines 65-67). The attack tree structures include root datasets that has a child dataset with a combination derived from and less granular than a root dataset. The child dataset of a root dataset is identified through the root dataset (col. 6, lines 25-66). The teachings of Schneier are silent in disclosing of a keysets that are included in the datasets. The examiner notes that a keyset is broadly interpreted as being data indicative of attack profiles as is recited in the applicant's specification on page 3, lines 6-7 and page 10, lines 17-21. It is disclosed by Conklin et al of network data is sent in the form of packets which include various identification information (keysets) that is used to transmit data for establishing and maintaining connections (col.

2, line 64 through col. 3, line 14). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply means of maintaining keyset data that indicates certain characteristics of network activity. Conklin et al recites motivation for the use of keysets by disclosing that these keysets, or descriptions, provide useful information when it comes to detection an intrusion since some of this information can become predictable (col. 4, line 61 through col. 5, line 9). It is obvious that since the teachings of Schneier are dedicated towards detecting attacks, the teachings would have been improved by tracking additional identification information, or keysets, that describes the patterns of attacks as is disclosed by Conklin et al.

As per claims 2,22, and 40, Schneier teaches of identifying child datasets of the root dataset through the root dataset (col. 6, lines 25-66 and as shown in Figure 3).

As per claims 3,23, and 41, it is taught by Schneier of identifying all child datasets of the root dataset through the root dataset (col. 6, lines 25-66 and as shown in Figure 3).

As per claims 4 and 24, Schneier discloses of identifying the child dataset of the root dataset with a pointer from the root dataset to the child dataset (col. 6, lines 25-66 and as shown in Figure 3).

As per claims 5,25, and 42, it is disclosed by Schneier of identifying all child datasets through their root datasets (col. 6, lines 25-66 and as shown in Figure 3).

As per claims 6 and 26, Schneier teaches that each root dataset comprises child datasets (col. 6, lines 25-66 and as shown in Figure 3).

As per claims 7,27, and 43, Schneier discloses that a root dataset includes sibling root datasets, the sibling root dataset and the root dataset having datasets that are the reverse order of each other and the sibling datasets can be identified through the root dataset (col. 6, lines 25-66 and as shown in Figure 3). The teachings of Conklin et al are relied upon for the disclosure of keysets, please refer above for the motivational benefits of applying Conklin et al to the teachings of Schneier.

As per claims 8 and 28, Schneier teaches of root datasets and the sibling root dataset collectively identify all of their child datasets and identify one another (col. 6, lines 25-66 and as shown in Figure 3).

As per claims 9 and 29, Conklin et al discloses of keysets comprising a source address and a destination address key (col. 3, lines 3-11 and col. 4, lines 61-67). Please refer above for the motivational benefits of applying Conklin et al to the teachings of Schneier.

As per claims 10 and 30, Conklin et al teaches of keysets comprising quad keysets (col. 3, lines 3-11 and col. 4, lines 61-67). Please refer above for the motivational benefits of applying Conklin et al to the teachings of Schneier.

As per claims 11 and 31, it is disclosed by Conklin et al that quad keysets comprise a source address key, a source port key, a destination address key, and a destination port key (col. 3, lines 3-11 and col. 4, lines 61-67). Please refer above for the motivational benefits of applying Conklin et al to the teachings of Schneier.

As per claims 12 and 32, Conklin et al teaches of keysets being single, dual, and triple keysets (col. 3, lines 3-11 and col. 4, lines 61-67). Please refer above for the motivational benefits of applying Conklin et al to the teachings of Schneier.

As per claims 13 and 33, Conklin et al teaches of keysets comprising steam keysets (col. 3, lines 3-11 and col. 4, lines 61-67). Please refer above for the motivational benefits of applying Conklin et al to the teachings of Schneier.

As per claims 14 and 34, it is disclosed by Conklin et al that stream based keysets comprise a source address key, a source port key, a destination address key, and a destination port key (col. 3, lines 3-11 and col. 4, lines 61-67). Please refer above for the motivational benefits of applying Conklin et al to the teachings of Schneier.

As per claims 15 and 35, it is disclosed by Schneier of data tree structures (datasets or buckets) for an intrusion detection system (col. 5, lines 65-67).

As per claim 16, Schneier teaches of identifying all child datasets of the root dataset through the root dataset with a single search of a database storing the datasets (col. 5, lines 65-67, col. 6, lines 25-66, and as shown in Figure 3).

As per claims 18,19,36,37, and 45, it is disclosed by Schneier of data tree structures (datasets or buckets) for an intrusion detection system (col. 5, lines 65-67). The examiner asserts that it is obvious that the outdated root datasets and child datasets, as indicated by a time stamp or counter, so that the outdated information can be removed since it is well known that databases are regularly maintained for efficiency purposes. The motivational benefits of removed outdated data allows the database to be more efficient for purposes of storage and retrieval.

As per claim 47, Schneier discloses of data tree structures (datasets) for an intrusion detection system (col. 5, lines 65-67). A plurality of pointers identify child datasets having combinations derived from, and less granular than the root (col. 6, lines 25-66). The teachings of Schneier are silent in disclosing of a keysets that are included in the datasets that are representative of a network connection. The examiner notes that a keyset is broadly interpreted as being data indicative of attack profiles as is recited in the applicant's specification on page 3, lines 6-7 and page 10, lines 17-21. It is disclosed by Conklin et al of network data is sent in the form of packets which include various identification information (keysets) that is used to transmit data for establishing and maintaining connections (col. 2, line 64 through col. 3, line 14). Conklin et al discloses of keysets comprising a source address and a destination address key (col. 3, lines 3-11 and col. 4, lines 61-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply means of maintaining keyset data that indicates certain characteristics of network activity. Conklin et al recites motivation for the use of keysets by disclosing that these keysets, or descriptions, provide useful information when it comes to detection an intrusion since some of this information can become predictable (col. 4, line 61 through col. 5, line 9). It is obvious that since the teachings of Schneier are dedicated towards detecting attacks, the teachings would have been improved by tracking additional identification information, or keysets, that describes the patterns of attacks as is disclosed by Conklin et al.

As per claim 48, Conklin et al teaches of a termination status indicator (col. 4, line 61 through col. 5, line 9). Please refer above for the motivational benefits of applying Conklin et al to the teachings of Schneier.

As per claim 49, it is disclosed by Schneier that a pointer identifies a sibling root dataset of the root dataset (col. 6, lines 25-66 and as shown in Figure 3).

Allowable Subject Matter

3. Claims 17,20,38,44, and 46 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

4. Claims 50 and 51 are allowed.

5. It was not found to be taught in the prior art of retrieving data for processing of a traffic signature by performing a single search for a root dataset having a quad keyset corresponding to the traffic signature and identifying relevant child and sibling root datasets through the pointers of the root dataset. The examiner notes that a keyset is broadly interpreted as being data indicative of attack profiles as is recited in the applicant's specification on page 3, lines 6-7 and page 10, lines 17-21.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gomez et al, "Complete Expression Trees for Evolving Fuzzy Classifier Systems with Genetic Algorithms and Application to Network Intrusion Detection"

Chang et al, "Parsimonious Downgrading and Decision Tree Applied to the Inference Problem"

Kumar, "Classification and Detection of Computer Intrusions"

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131
AU2131
12/12/04

CR

December 12, 2004